

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-345795

(43)Date of publication of application : 14.12.2001

(51)Int.Cl.

H04L 9/08

H04B 7/26

H04Q 7/38

(21)Application number : 2000-161687

(71)Applicant : SONY CORP

(22)Date of filing : 31.05.2000

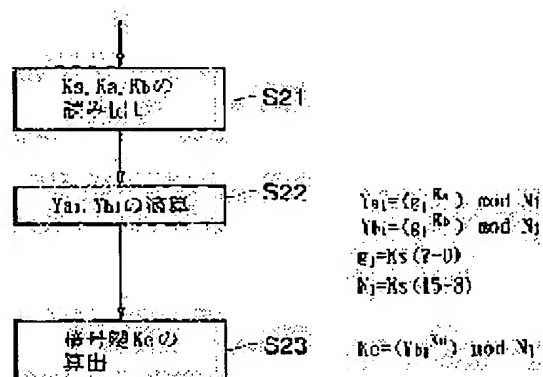
(72)Inventor : MAEKAWA TAKUJI

(54) APPARATUS AND METHOD FOR RADIO COMMUNICATION

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an apparatus and a method for radio communication in which tapping or interception can be prevented by a relatively convenient method in a closed environment where the counterpart of communication is somewhat limited, e.g. wireless LAN in home or company.

SOLUTION: A private key ka for use in its own radio communication unit and a private key kb for use in a counterpart radio communication unit are exchanged. The transmission signal processing section in a transmitter calculates an encryption key ke using a common secret key ks for common use in a radio communication system and the private keys ka, kb and encrypts data to be transmitted using a calculated encryption key ke. The private keys ka, kb are secret even for other users in the radio communication system. Consequently, an encryption key employing the private keys ka, kb, has high secrecy. The encryption key ke can be calculated using a simple algorithm.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-345795

(P2001-345795A)

(43) 公開日 平成13年12月14日 (2001. 12. 14)

(51) Int.Cl.⁷

識別記号

F I

テーマコード(参考)

H 0 4 L 9/08

H 0 4 L 9/00

6 0 1 C 5 J 1 0 4

H 0 4 B 7/26

H 0 4 B 7/26

M 5 K 0 6 7

H 0 4 Q 7/38

1 0 9 R

H 0 4 L 9/00

6 0 1 E

審査請求 未請求 請求項の数17 O L (全 12 頁)

(21) 出願番号 特願2000-161687(P2000-161687)

(22) 出願日 平成12年5月31日(2000. 5. 31)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 前川 卓司

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100094053

弁理士 佐藤 隆久

Fターム(参考) 5J104 AA16 EA24 EA28 EA33 NA02

NA03 NA18

5K067 AA30 BB02 BB21 GG01 GG11

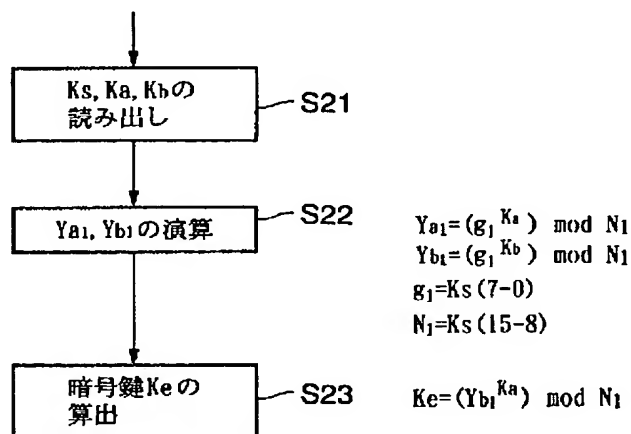
HH24

(54) 【発明の名称】 無線通信装置および無線通信方法

(57) 【要約】

【課題】 家庭内無線LAN、企業内無線LANなどのようにある程度通信相手が限定されており閉じられた環境における無線通信において、比較的簡易な方法で、盗聴、傍受出来ない無線通信装置、無線通信方法を提供する。

【解決手段】 自己の無線通信装置に用いる秘密鍵 k_a と、送信相手となる無線通信装置に用いるユーザの秘密鍵 k_b とを交換する。送信機の送信信号処理部は、無線通信システムに共通に用いる共通秘密鍵 k_s と、秘密鍵 k_a と、秘密鍵 k_b とを用いて暗号化鍵 k_e を算出し、算出した暗号化鍵 k_e を用いて送信すべきデータを暗号処理する。秘密鍵 k_a および秘密鍵 k_b は、無線通信システム内の他のユーザにも秘密である。したがって、秘密鍵 k_a および秘密鍵 k_b を用いた暗号化鍵は機密性が高い。その一方、暗号化鍵 k_e の算出は簡単なアルゴリズムで行うことができる。



1

【特許請求の範囲】

【請求項 1】自己の無線通信装置に用いる第 1 のユーザ秘密鍵と、送信相手となる無線通信装置に用いる第 2 のユーザ秘密鍵と、その無線通信システムに共通に用いる共通秘密鍵とを用いて演算を行って暗号化鍵を算出する暗号化鍵算出手段と、

上記算出した暗号化鍵を用いて送信すべきデータを暗号処理する暗号処理手段と、

上記暗号処理されたデータを送出する送出手段とを有する送信機を具備する無線通信装置。

【請求項 2】上記送信機内の上記暗号化鍵算出手段は、上記共通秘密鍵から導出した第 1 の鍵算出用因子と上記第 2 のユーザの秘密鍵とを用いた演算を行い、その結果

$$Y_b = (g^{K_b}) \bmod N$$

$$k_e = (Y_b^{K_a}) \bmod N$$

ただし、 k_e は暗号化鍵であり、

Y_b は鍵算出用パラメータであり、

g は共通秘密鍵から導出した第 1 の鍵算出用因子であり、

N は共通秘密鍵から導出した第 2 の鍵算出用因子であり、

k_a は第 1 の秘密鍵であり、

k_b は第 2 の秘密鍵である。

【請求項 4】自己の無線通信装置に用いる第 1 のユーザ秘密鍵と、送信相手となる無線通信装置に用いる第 2 のユーザ秘密鍵と、その無線通信システムに共通に用いる共通秘密鍵とを用いて演算を行って暗号解読鍵を算出する暗号解読鍵算出手段と、

上記算出した暗号解読鍵を用いて受信したデータを暗号解読処理する暗号解読処理手段とを有する受信機を具備する無線通信装置。

$$Y_b = (g^{K_b}) \bmod N$$

$$k_e = (Y_b^{K_a}) \bmod N$$

ただし、 k_e は暗号解読鍵であり、

Y_b は鍵算出用パラメータであり、

g は共通秘密鍵から導出した第 1 の鍵算出用因子であり、

N は共通秘密鍵から導出した第 2 の鍵算出用因子であり、

k_a は第 1 の秘密鍵であり、

k_b は第 2 の秘密鍵である。

【請求項 7】自己の無線通信装置に用いる第 1 のユーザ秘密鍵と、送信相手となる無線通信装置に用いる第 2 のユーザ秘密鍵と、その無線通信システムに共通に用いる共通秘密鍵とを用いて演算を行って暗号化鍵を算出する暗号化鍵算出手段と、

上記算出した暗号化鍵を用いて送信すべきデータを暗号処理する暗号処理手段と、

上記暗号処理されたデータを送出する送出手段とを有する送信機と、

2

を上記共通秘密鍵から導出した上記第 1 の鍵算出用因子とは異なる第 2 の鍵算出用因子を用いて演算する第 1 の演算手段と、

上記第 1 の演算手段における演算結果について自己のユーザの秘密鍵とを用いた演算を行い、その結果を上記共通秘密鍵から導出した上記第 2 の鍵算出用因子を用いて演算して上記暗号化鍵を算出する第 2 の演算手段とを有する、請求項 1 記載の無線通信装置。

【請求項 3】上記第 1 の演算手段における演算は下記式

10 A により行い、

上記第 2 の演算手段における演算は下記式 B により行う請求項 2 記載の無線通信装置。

$$\dots (A)$$

$$\dots (B)$$

【請求項 5】上記受信機内の上記暗号解読鍵算出手段は、

上記共通秘密鍵から導出した第 1 の鍵算出用因子と上記第 2 のユーザの秘密鍵とを用いた演算を行い、その結果を上記共通秘密鍵から導出した上記第 1 の鍵算出用因子とは異なる第 2 の鍵算出用因子を用いて演算する第 1 の演算手段と、

20

上記第 1 の演算手段における演算結果について自己のユーザの秘密鍵とを用いた演算を行い、その結果を上記共通秘密鍵から導出した上記第 2 の鍵算出用因子を用いて演算して上記暗号解読鍵を算出する第 2 の演算手段とを有する、請求項 4 記載の無線通信装置。

【請求項 6】上記第 1 の演算手段における演算は下記式 C により行い、

30

上記第 2 の演算手段における演算は下記式 D により行う請求項 5 記載の無線通信装置。

$$\dots (C)$$

$$\dots (D)$$

上記第 1 のユーザ秘密鍵と、上記第 2 のユーザ秘密鍵と、上記共通秘密鍵とを用いて演算を行って暗号解読鍵を算出する暗号解読鍵算出手段と、

上記算出した暗号解読鍵を用いて受信したデータを暗号解読処理する暗号解読処理手段とを有する受信機とを具備する無線通信装置。

40

【請求項 8】上記送信機内の上記暗号化鍵算出手段は、上記共通秘密鍵から導出した第 1 の鍵算出用因子と上記第 2 のユーザの秘密鍵とを用いた演算を行い、その結果を上記共通秘密鍵から導出した上記第 1 の鍵算出用因子とは異なる第 2 の鍵算出用因子を用いて演算する第 1 の演算手段と、

上記第 1 の演算手段における演算結果について自己のユーザの秘密鍵とを用いた演算を行い、その結果を上記共通秘密鍵から導出した上記第 2 の鍵算出用因子を用いて演算して上記暗号化鍵を算出する第 2 の演算手段とを有し、

50

3

上記受信機内の上記暗号解読鍵算出手段は、
 上記共通秘密鍵から導出した第1の鍵算出用因子と上記
 第2のユーザの秘密鍵とを用いた演算を行い、その結果
 を上記共通秘密鍵から導出した上記第1の鍵算出用因子
 とは異なる第2の鍵算出用因子を用いて演算する第3の
 演算手段と、
 上記第3の演算手段における演算結果について自己のユ
 ーザの秘密鍵とを用いた演算を行い、その結果を上記共
 通秘密鍵から導出した上記第2の鍵算出用因子を用いて

$$Y_b = (g^{K_b}) \bmod N$$

$$k_e = (Y_b^{K_a}) \bmod N$$

ただし、 k_e は暗号化鍵であり、
 Y_b は鍵算出用パラメータであり、
 g は共通秘密鍵から導出した第1の鍵算出用因子であ
 り、
 N は共通秘密鍵から導出した第2の鍵算出用因子であ
 り、

$$Y_a = (g^{K_a}) \bmod N$$

$$k_e = (Y_a^{K_b}) \bmod N$$

ただし、 k_e は暗号解読鍵であり、
 Y_b は鍵算出用パラメータであり、
 g は共通秘密鍵から導出した第1の鍵算出用因子であ
 り、
 N は共通秘密鍵から導出した第2の鍵算出用因子であ
 り、

$$Y_a = (g^{K_a}) \bmod N$$

$$k_e = (Y_a^{K_b}) \bmod N$$

ただし、 k_e は暗号解読鍵であり、
 Y_b は鍵算出用パラメータであり、
 g は共通秘密鍵から導出した第1の鍵算出用因子であ
 り、
 N は共通秘密鍵から導出した第2の鍵算出用因子であ
 り、
 k_a は第1の秘密鍵であり、
 k_b は第2の秘密鍵である。

【請求項12】第1の無線通信装置に用いる第1のユー
 ザ秘密鍵と、第2の無線通信装置に用いる第2のユーザ
 秘密鍵と、その無線通信システムに共通に用いる共通秘
 密鍵とを交換する工程と、
 送信する際、上記共通秘密鍵、第1のユーザの秘密鍵お
 よび第2のユーザの秘密鍵を用いて演算を行って暗号化鍵
 を算出する工程と、
 上記算出した暗号化鍵を用いて送信すべきデータを暗号
 処理する暗号処理工程と、

$$Y_b = (g^{K_b}) \bmod N$$

$$k_e = (Y_b^{K_a}) \bmod N$$

ただし、 k_e は暗号化鍵であり、
 Y_b は鍵算出用パラメータであり、
 g は共通秘密鍵から導出した第1の鍵算出用因子であ
 り、

4

演算して上記暗号解読鍵を算出する第4の演算手段とを
 有する、
 請求項7記載の無線通信装置。

【請求項9】上記第1の演算手段における演算は下記式
 Eにより行い、
 上記第2の演算手段における演算は下記式Fにより行
 う、
 請求項8記載の無線通信装置。

$$\dots (E)$$

$$\dots (F)$$

k_a は第1の秘密鍵であり、
 k_b は第2の秘密鍵である。

【請求項10】上記第3の演算手段における演算は下記
 式Gにより行い、
 上記第4の演算手段における演算は下記式Hにより行
 う
 請求項8記載の無線通信装置。

$$\dots (G)$$

$$\dots (H)$$

20 k_a は第1の秘密鍵であり、
 k_b は第2の秘密鍵である。

【請求項11】上記第3の演算手段における演算は下記
 式Gにより行い、
 上記第4の演算手段における演算は下記式Hにより行
 う
 請求項9記載の無線通信装置。

$$\dots (G)$$

$$\dots (H)$$

上記暗号処理されたデータを送出する送出工程とを有す
 る無線通信方法。

30 【請求項13】上記送信機内の上記暗号化鍵算出工程
 は、

上記共通秘密鍵から導出した第1の鍵算出用因子と上記
 第2のユーザの秘密鍵とを用いた演算を行い、その結果
 を上記共通秘密鍵から導出した上記第1の鍵算出用因子
 とは異なる第2の鍵算出用因子を用いて演算する第1の
 演算工程と、上記第1の演算工程における演算結果につ
 いて自己のユーザの秘密鍵とを用いた演算を行い、その
 結果を上記共通秘密鍵から導出した上記第2の鍵算出用
 因子を用いて演算して上記暗号化鍵を算出する第2の演
 算工程とを有する、請求項12記載の無線通信方法。

【請求項14】上記第1の演算工程における演算は下記
 式Iにより行い、
 上記第2の演算工程における演算は下記式Jにより行
 う
 請求項13記載の無線通信方法。

$$\dots (I)$$

$$\dots (J)$$

N は共通秘密鍵から導出した第2の鍵算出用因子であ
 り、

k_a は第1の秘密鍵であり、

50 k_b は第2の秘密鍵である。

5

【請求項 15】第 1 の無線通信装置に用いる第 1 のユーザ秘密鍵と、第 2 の無線通信装置に用いる第 2 のユーザ秘密鍵と、その無線通信システムに共通に用いる共通秘密鍵とを交換する工程と、

信号を受信した際、上記第 1 のユーザ秘密鍵と、上記第 2 のユーザ秘密鍵と、上記共通秘密鍵とを用いて演算を行って暗号解読鍵を算出する暗号解読鍵算出工程と、上記算出した暗号解読鍵を用いて受信したデータを暗号解読処理する暗号解読処理工程とを有する、無線通信方法。

【請求項 16】上記暗号解読鍵算出工程は、上記共通秘密鍵から導出した第 1 の鍵算出用因子と上記第 2 のユーザの秘密鍵とを用いた演算を行い、その結果

$$Y_b = (g^{K_b})_{\text{mod}N}$$

$$k_o = (Y_b^{K_a})_{\text{mod}N}$$

ただし、 k_o は暗号解読鍵であり、 Y_b は鍵算出用パラメータであり、 g は共通秘密鍵から導出した第 1 の鍵算出用因子であり、 N は共通秘密鍵から導出した第 2 の鍵算出用因子であり、 K_a は第 1 の秘密鍵であり、 K_b は第 2 の秘密鍵である。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、無線通信システムにおける無線通信装置および無線通信方法に関するものであり、特に、家庭内無線局領域ネットワーク (Local Area Network: LAN)、企業内無線 LAN などのように、通信相手がある程度限定されている無線通信環境において暗号処理方法および復号処理方法を行う無線通信装置および無線通信方法に関する。

【0002】

【従来の技術】無線通信方式においては無線信号が空中を伝搬するから第三者に盗聴、傍受される可能性が高い。そして、傍受後、故意または悪意の第三者によってデータの改ざんなどが行われる場合もある。

【0003】一般的な無線通信システムにおいては、そのような盗聴、傍受、そして、改ざんを防止するため、データを暗号処理した後、データ無線送信し、受信側で暗号を解いてデータを復元している。

【0004】また、家庭内無線 LAN、企業内無線 LAN など、ある程度閉じられた無線通信環境における盗聴、傍受防止対策としては、IC カードのメモリに記録された認証 (ID) 番号 (または ID コード) を用いる場合が多い。

【0005】

【発明が解決しようとする課題】家庭内無線 LAN、企業内無線 LAN など一般的な無線通信システムにおける暗号処理、復号処理を適用すると、処理が複雑になる

6

を上記共通秘密鍵から導出した上記第 1 の鍵算出用因子とは異なる第 2 の鍵算出用因子を用いて演算する第 1 の演算工程と、

上記第 1 の演算工程における演算結果について自己のユーザの秘密鍵とを用いた演算を行い、その結果を上記共通秘密鍵から導出した上記第 2 の鍵算出用因子を用いて演算して上記暗号解読鍵を算出する第 2 の演算工程とを有する、請求項 15 記載の無線通信方法。

【請求項 17】上記第 1 の演算工程における演算は下記式 K により行い、

上記第 2 の演算手段における演算は下記式 L により行う請求項 16 記載の無線通信方法。

$$\dots (K)$$

$$\dots (L)$$

という問題がある。

【0006】家庭内無線 LAN、企業内無線 LAN に ID 番号などを用いた場合も、処理が複雑になるという問題があった。また、一旦、ID 番号が格納されている IC カードが盗用されて ID 番号が第 3 者に知得された場合、暗号化データの改ざんが行われる可能性がある。そのような事態を知ったとき、ID 番号が格納されたか IC カードの再発行が必要になるが、IC カードの再発行は手続きが複雑であるし、価格的にも高額になるので、家庭内無線 LAN、企業内無線 LAN などへの ID 番号を格納した IC カードを適用することは不都合な場合が多い。

【0007】本発明の目的は、家庭内無線 LAN、企業内無線 LAN などのように、ある程度通信相手が限定されており閉じられた環境における無線通信において、比較的簡易な方法で、盗聴、傍受、さらに改ざんなどが起きない無線通信装置を提供することにある。本発明の他の目的は、上記無線通信装置に適用する無線通信方法を提供することにある。

【0008】

【課題を解決するための手段】本発明の第 1 の観点によれば、自己の無線通信装置に用いる第 1 のユーザ秘密鍵と、送信相手となる無線通信装置に用いる第 2 のユーザ秘密鍵と、その無線通信システムに共通に用いる共通秘密鍵とを用いて演算を行って暗号化鍵を算出する暗号化鍵算出手段と、上記算出した暗号化鍵を用いて送信すべきデータを暗号処理する暗号処理手段と、上記暗号処理されたデータを送出する送出手段とを有する送信機を具備する無線通信装置が提供される。

【0009】上記送信機内の上記暗号化鍵算出手段は、上記共通秘密鍵から導出した第 1 の鍵算出用因子と上記第 2 のユーザの秘密鍵とを用いた演算を行い、その結果を上記共通秘密鍵から導出した上記第 1 の鍵算出用因子とは異なる第 2 の鍵算出用因子を用いて演算する第 1 の演算手段と、上記第 1 の演算手段における演算結果につ

いて自己のユーザの秘密鍵とを用いた演算を行い、その結果を上記共通秘密鍵から導出した上記第2の鍵算出用因子を用いて演算して上記暗号化鍵を算出する第2の演算手段とを有する。

$$Y_b = (g^{K_b})_{\text{mod}N}$$

$$k_e = (Y_b^{K_a})_{\text{mod}N}$$

【0012】ただし、 k_e は暗号化鍵であり、 Y_b は鍵算出用パラメータであり、 g は共通秘密鍵から導出した第1の鍵算出用因子であり、 N は共通秘密鍵から導出した第2の鍵算出用因子であり、 k_a は第1の秘密鍵であり、 k_b は第2の秘密鍵である。

【0013】また本発明によれば、自己の無線通信装置に用いる第1のユーザ秘密鍵と、送信相手となる無線通信装置に用いる第2のユーザ秘密鍵と、その無線通信システムに共通に用いる共通秘密鍵とを用いて演算を行って暗号解読鍵を算出する暗号解読鍵算出手段と、上記算出した暗号解読鍵を用いて受信したデータを暗号解読処理する暗号解読処理手段とを有する受信機を具備する無線通信装置が提供される。

【0014】上記受信機内の上記暗号解読鍵算出手段

$$Y_b = (g^{K_b})_{\text{mod}N}$$

$$k_e = (Y_b^{K_a})_{\text{mod}N}$$

【0017】ただし、 k_e は暗号解読鍵であり、 Y_b は鍵算出用パラメータであり、 g は共通秘密鍵から導出した第1の鍵算出用因子であり、 N は共通秘密鍵から導出した第2の鍵算出用因子であり、 k_a は第1の秘密鍵であり、 k_b は第2の秘密鍵である。

【0018】本発明によれば、上記送信機と上記受信機とを有する無線通信装置が提供される。

【0019】本発明によれば、上記送信機で行う無線通信方法が提供される。当該無線通信方法は、第1の無線通信装置に用いる第1のユーザ秘密鍵と、第2の無線通信装置に用いる第2のユーザ秘密鍵と、その無線通信システムに共通に用いる共通秘密鍵とを交換する工程と、送信する際、上記共通秘密鍵、第1のユーザの秘密鍵および第2のユーザの秘密鍵を用いて演算を行って暗号化鍵を算出する工程と、上記算出した暗号化鍵を用いて送信すべきデータを暗号処理する暗号処理工程と、上記暗号処理されたデータを送出する送出工程とを有する。

【0020】また本発明によれば、上記受信機で行う無線通信方法が提供される。当該無線通信方法は、第1の無線通信装置に用いる第1のユーザ秘密鍵と、第2の無線通信装置に用いる第2のユーザ秘密鍵と、その無線通信システムに共通に用いる共通秘密鍵とを交換する工程と、信号を受信した際、上記第1のユーザ秘密鍵と、上記第2のユーザ秘密鍵と、上記共通秘密鍵とを用いて演算を行って暗号解読鍵を算出する暗号解読鍵算出工程と、上記算出した暗号解読鍵を用いて受信したデータを暗号解読処理する暗号解読処理工程とを有する。

【0021】本発明の無線通信装置および無線通信方法

【0010】特定的には、上記第1の演算手段における演算は下記式Aにより行い、上記第2の演算手段における演算は下記式Bにより行う。

【0011】

・・・(A)

・・・(B)

は、上記共通秘密鍵から導出した第1の鍵算出用因子と上記第2のユーザの秘密鍵とを用いた演算を行い、その結果を上記共通秘密鍵から導出した上記第1の鍵算出用因子とは異なる第2の鍵算出用因子を用いて演算する第1の演算手段と、上記第1の演算手段における演算結果について自己のユーザの秘密鍵とを用いた演算を行い、その結果を上記共通秘密鍵から導出した上記第2の鍵算出用因子を用いて演算して上記暗号解読鍵を算出する第2の演算手段とを有する。

【0015】上記第1の演算手段における演算は下記式Cにより行い、上記第2の演算手段における演算は下記式Dにより行う。

【0016】

・・・(C)

・・・(D)

は、無線通信システムの有効なユーザに対して共通秘密鍵を配付する。そして、通信相手相互に第1のユーザの秘密鍵 k_a と第2のユーザの秘密鍵 k_b との交換を行う。これら第1のユーザの秘密鍵 k_a と第2のユーザの秘密鍵 k_b の交換は、通信相手同士の交換であり、無線通信システムのユーザに対しては秘密である。したがって、同じ無線通信システムに属しても通信相手の当事者以外には秘密の鍵であり、鍵の機密性は高い。無線通信装置において送信する場合、共通秘密鍵から導出した第1の鍵算出用因子と第2の鍵算出用因子と、第1および第2のユーザ秘密鍵を用いて暗号化鍵を算出する。この暗号化鍵を用いて送信データを暗号処理すれば、ユーザ秘密鍵を交換して相手しか解読できない機密性の高い送信信号となる。したがって、無線通信システムにおいて傍受されたとしても、意味不明の信号となる。

【0022】暗号化鍵の算出アルゴリズムは比較的簡単である。

【0023】

【発明の実施の形態】図1は本発明の無線通信装置および無線通信方法が適用される無線通信システムの構成例を示す図であり、無線通信システムとしては、たとえば、企業内無線LANまたは家庭内無線LANである。以下、無線通信システムとして企業内無線LANを例示して述べる。図1に図解した企業内無線LANにおいては、3個の無線通信端末装置1～3が相互に通信可能な状態にある。このような通信環境において、本実施の形態においては、二人の利用者（ユーザ）U1、U2が上記無線通信端末装置1～3を利用可能な状態にある。し

かしながら、本実施の形態において、ユーザが相互に無線通信を行う場合、送信すべきデータ（以下、送信データ）に鍵を用いた暗号処理をする。そのため、各ユーザは事前に自己の鍵を持ち、かつ、通信相手（通信相手となるユーザ）と相互に鍵の交換をしておく。

【0024】本実施の形態における使用する鍵とその交換について述べる。無線通信システムにおいて、無線通信端末装置1～3を使用して通信可能な全てのユーザには、無線通信システムに共通の秘密鍵 k_s （以下、共通秘密鍵 k_s ）が事前に通知される。さらに、通信を行う第1のユーザU1と第2のユーザU2とは、事前に、互いに自己の秘密鍵を相手に通知しておく。ここでは、ユーザU1の秘密鍵を k_a として、ユーザU2の秘密鍵を k_b とする。すなわち、ユーザU1は自己の秘密鍵 k_a をユーザU2に通知し、ユーザU2は自己の秘密鍵 k_b をユーザU2に通知しておく。したがって、ユーザU1は、共通秘密鍵 k_s と、自己の秘密鍵 k_a とに加えて、通信相手であるユーザU2の秘密鍵 k_b とを持つ。同様に、ユーザU2は、共通秘密鍵 k_s と、自己の秘密鍵 k_b とに加えて、通信相手であるユーザU1の秘密鍵 k_a とを持つ。もちろん、この無線通信システムにおいて第3者であるユーザU3に対しては、上記鍵は秘密の状態にしておく。

【0025】図2は図1に図解した無線通信システムにおける無線通信端末装置の構成例を示す図である。無線通信端末装置1は、送信機10と、受信機20と、共通部30とを有する。送信機10は、送信データ入力部12と、送信信号処理部14と、周波数変換部16と、送信部18とを有する。受信機20は、受信部22と、周波数変換部24と、受信信号処理部26と、復号信号出力部28とを有する。共通部30は、送受信アンテナ32と、アンテナ切り換え部34と、送受信信号処理部36とを有する。

【0026】なお、無線通信端末装置2～3の構成も基本的には、無線通信端末装置1の構成と同様であるから、無線通信端末装置2～3の構成については図解を省略し、その説明を割愛する。

【0027】図3を参照して無線通信端末装置1における送信動作を述べる。

【0028】ステップ1：送信データ入力部12は、送受信信号処理部36から送信すべきデータ（送信データ）を入力して、送信信号処理部14に送出する。

【0029】ステップ2：送信信号処理部14は、送信データについて暗号処理して、さらに必要に応じて、暗号処理した送信データを符号化し、変調処理する。暗号処理については図5を参照して後述する。符号化処理の例としては、たとえば、画像データについてMPEG、JPEGなどにより圧縮する。符号化処理の他の例として、音声データのみの場合にはCODECによる音声圧縮処理をする。変調処理としては、たとえば、FM変調、

QAM変調処理などを行う。

【0030】ステップ3：周波数変換部16は、送信信号処理部14で処理したベースバンドの信号を中間周波数の信号に変換し、さらには無線送信可能な高周波信号に変換する。このように、周波数変換部16はベースバンドの周波数信号を高周波信号にアップコンバートする。

【0031】ステップ4：送信部18は、周波数変換部16で高周波信号に変換された信号を電力増幅などを行い、送受信アンテナ32を介して空中に電波として放射する。このとき、アンテナ切り換え部34は送受信アンテナ32と送信部18とが接続されるように切り換えられている。

【0032】図4を参照して無線通信端末装置1における受信動作を述べる。

【0033】ステップ5：上述した方法で無線通信端末装置2～3のいずれかの無線通信端末装置から電波が放射されたとき、送受信アンテナ32はその電波を受信する。この受信モードのとき、送受信アンテナ32は受信部22に接続されるように切り換えられている。したがって、送受信アンテナ32で受信した電波信号は受信部22に印加される。受信部22は微弱な送受信アンテナ32で検出した電気信号を増幅して周波数変換部24に送出する。

【0034】ステップ6：周波数変換部24は周波数変換部16と逆の動作を行う。すなわち、周波数変換部24は、高周波受信信号を中間周波信号に変換し、ベースバンド信号に変換する。このように、周波数変換部24は高周波信号をベースバンドの周波数信号にダウンコンバートする。

【0035】ステップ7：受信信号処理部26は、ベースバンドの受信信号について、送信信号処理部14と逆の動作を行う。すなわち、受信信号処理部26は、周波数変換部24の出力信号を復調し、暗号化されているその結果を解読し、解読した結果を復号する。受信信号処理部26における復調は送信信号処理部14における変調の逆の処理をする。受信信号処理部26における暗号解読処理は送信信号処理部14における暗号処理と逆の処理になるが、その詳細は後述する。受信信号処理部26における復号は送信信号処理部14における符号化の逆の処理をする。

【0036】ステップ8：復号信号出力部28は、暗号を解読した結果を送受信信号処理部36に送出する。

【0037】以下、ユーザU1が無線通信端末装置1を用い、ユーザU2が無線通信端末装置2を用いて相互に通信を行う場合の、無線通信端末装置1の送信信号処理部14の動作のうち（図3、ステップ2）暗号処理、および、無線通信端末装置2の受信信号処理部（無線通信端末装置1の受信信号処理部26と同じ）の動作のうち（図4、ステップ7）、暗号解読処理について述べる。

【0038】図1を参照して鍵の交換について述べたように、第1のユーザU1と第2のユーザU2とは、事前に、共通秘密鍵 k_s を知り、互いに自己の秘密鍵を相手に通知しておく。ユーザU1の秘密鍵を k_a とし、ユーザU2の秘密鍵を k_b とする。このようにして交換された鍵は、無線通信端末装置1の送信信号処理部14および受信信号処理部26の共通のメモリ、および、無線通信端末装置2の送信信号処理部（無線通信端末装置1の送信信号処理部14と同じ）および受信信号処理部（無線通信端末装置1の受信信号処理部26と同じ）の共通のメモリに保存されているとする。すなわち、無線通信端末装置1のメモリには、共通秘密鍵 k_s と、自己の秘密鍵 k_a と、ユーザU2の秘密鍵 k_b とが保存されている。同様に、無線通信端末装置2のメモリには、共通秘密鍵 k_s と、自己の秘密鍵 k_b と、ユーザU1の秘密鍵 k_a とが保存されている。

【0039】なお、共通秘密鍵 k_s と秘密鍵 k_a は無線通信端末装置1のメモリに記憶しておき、共通秘密鍵 k_s と秘密鍵 k_b は無線通信端末装置2のメモリに記憶しておくが、通信相手の秘密鍵、すなわち、ユーザU2の秘密鍵 k_b は無線通信端末装置1のメモリに記憶させず、同様に、ユーザU1の秘密鍵 k_a を無線通信端末装置2のメモリには記憶させず、通信を行うとき、ユーザが送信信号処理部14に設定してもよい。その理由は、

$$\begin{aligned} Y_{a1} &= (g_1^{K_a}) \bmod N_1 \\ Y_{b1} &= (g_1^{K_b}) \bmod N_1 \end{aligned}$$

【0047】ただし、 Y_{a1} は第1の鍵算出用パラメータであり、 Y_{b1} は第2の鍵算出用パラメータであり、 g_1 は第1の鍵算出用因子であり、 N_1 は第2の鍵算出用因子であり、 k_a はユーザU1の秘密鍵であり、 k_b はユーザU2の秘密鍵である。

【0048】式1における $\bmod N_1$ は、 $(g_1^{K_a})$ の N_1 のモジュラス(modulus)を意味する。すなわち、式1における $\bmod N_1$ は $(g_1^{K_a})$ を N_1 で除算した結果の整数値を示す。同様に、式2における $\bmod N_1$ は、 $(g_1^{K_b})$ の N_1 のモジュラスを意味する。すなわち、式2における $\bmod N_1$ は $(g_1^{K_b})$ を N_1 で除算した結果の整数値を示す。

$$k_e = (Y_{b1}^{K_a}) \bmod N_1$$

【0052】第2の鍵算出用パラメータ Y_{b1} は式2において、共通秘密鍵 k_s の下位1バイトの数値である第1の鍵算出用因子 g_1 と、ユーザU2の秘密鍵 k_b とを用いて、 $(g_1^{K_b})$ を演算し、さらにその結果について $\bmod N_1$ （第2の鍵算出用因子 N_1 は共通秘密鍵 k_s の上位1バイトの数値）をとった値として算出されている。式3で規定される暗号化鍵 k_e は、そのような第2の鍵算出用パラメータ Y_{b1} に自己の秘密鍵 k_a の値でべき乗し、その結果について $\bmod N_1$ をとった値として算出される。以上のように、暗号化鍵 k_e は、共通秘密鍵 k_s （第1の鍵算出用因子 g_1 と第2の鍵算出用因子

通信相手（ユーザ）の秘密鍵を知らない第3者が勝手に暗号処理したデータの通信を行えなくするためである。

【0040】ただし、下記の実施の形態においては、無線通信端末装置1のメモリに、共通秘密鍵 k_s と、秘密鍵 k_a と、ユーザU2の秘密鍵 k_b とが保存されており、無線通信端末装置2のメモリに、共通秘密鍵 k_s と、秘密鍵 k_b と、ユーザU1の秘密鍵 k_a とが保存されている場合について述べる。

【0041】図5を参照して、無線通信端末装置1の送信信号処理部14における暗号処理について述べる。

【0042】ステップ11：送信信号処理部14は、メモリに記憶されている、共通秘密鍵 k_s と、自己の秘密鍵 k_a と、ユーザU2の秘密鍵 k_b とを用いて、暗号処理に使用する暗号化鍵 k_e を導出する。暗号化鍵 k_e の導出方法については、図6を参照して詳述する。

【0043】図6は暗号化鍵 k_e の導出方法を示すフローチャートである。

【0044】ステップ21：無線通信端末装置1の送信信号処理部14は、メモリに記憶されている共通秘密鍵 k_s と、自己の秘密鍵 k_a と、通信相手であるユーザU2の秘密鍵 k_b とをメモリから検索して読みだす。

【0045】ステップ22：送信信号処理部14は、下記演算を行う。

$$\begin{aligned} \text{【0046】} & \dots (1) \\ & \dots (2) \end{aligned}$$

【0049】第1の鍵算出用因子 g_1 および第2の鍵算出用因子 N_1 について述べる。たとえば、共通秘密鍵 k_s が2バイトのとき、第1の鍵算出用因子 g_1 は共通秘密鍵 k_s の下位1バイトのデータ、すなわち、共通秘密鍵 k_s の(7-0)ビットのデータである。また、第2の鍵算出用因子 N_1 は共通秘密鍵 k_s の上位1バイトのデータ、すなわち、暗号化鍵 k_e の(15-8)ビットのデータである。

【0050】ステップ23：送信信号処理部14は下記の演算により暗号化鍵 k_e を算出する。

$$\text{【0051】} \dots (3)$$

N_1 として使用)、自己の秘密鍵 k_a と、送信相手であるユーザU2の秘密鍵 k_b とを用いて算出される。

【0053】図5を再び、参照して送信信号処理部14の動作を述べる。ステップ12：送信信号処理部14は暗号化鍵 k_e を算出した場合、その暗号化鍵 k_e を用いて送信すべきデータを暗号処理する。暗号化鍵 k_e を用いるデータの暗号処理態は公知の処理を適用できる。このようにして暗号処理された送信データが、図3のステップ2において、符号化され、変調された後、周波数変換部16で周波数変換され、送信部18において増幅され、送受信アンテナ32を介して電波として放射され

る。

【0054】図7を参照して、上述した暗号処理された信号を受信して無線通信端末装置2における暗号解読処理について述べる。無線通信端末装置2の内部構成は、図2に図解した無線通信端末装置1の構成と同じである。したがって、無線通信端末装置2の受信処理は、図4を参照して述べた受信機20の処理と同様であり、暗号解読処理も、受信機20内の受信信号処理部26における処理と同様になる。そこで、図2に図解した受信機20における受信信号処理部26を参照して、無線通信端末装置2内の受信信号処理部の処理について述べる。受信信号処理部26は、図4のステップ7の処理として下記の動作を行う。

【0055】ステップ31：受信信号処理部26は、メモリに記憶されている、共通秘密鍵 k_s と、自己の秘密

$$Y_{a2} = (g_2^{K_a}) \bmod N_2$$

$$Y_{b2} = (g_2^{K_b}) \bmod N_2$$

【0060】ただし、 Y_{a2} は第1の鍵算出用パラメータであり、 Y_{b2} は第2の鍵算出用パラメータであり、 g_2 は第1の鍵算出用因子であり、 N_2 は第2の鍵算出用因子であり、 k_a はユーザU1の秘密鍵であり、 k_b はユーザU2の秘密鍵である。

【0061】式1における $\bmod N_2$ は、 $(g_1^{K_a})$ の N_2 のモジュラス(modulus)を意味する。すなわち、式1における $\bmod N_2$ は $(g_2^{K_a})$ を N_2 で除算した結果の整数値を示す。同様に、式2における $\bmod N_2$ は、 $(g_2^{K_b})$ の N_2 のモジュラスを意味する。すなわち、式2における $\bmod N_2$ ($g_2^{K_b})$ を N_2 で除算した結果の整数値を示す。

【0062】第1の鍵算出用因子 g_2 および第2の鍵算出用因子 N_2 について述べる。たとえば、共通秘密鍵 k_s が2バイトのとき、第1の鍵算出用因子 g_2 は共通秘

$$k_e = (Y_{a2}^{K_b}) \bmod N_2$$

【0066】第2の鍵算出用パラメータ Y_{a2} は式2において、共通秘密鍵 k_s の下位1バイトの数値である第1の鍵算出用因子 g_2 と、送信相手であるユーザU1の秘密鍵 k_a とを用いて、 $(g_2^{K_a})$ を演算し、さらにその結果について $\bmod N_2$ (第2の鍵算出用因子 N_2 は共通秘密鍵 k_s の上位1バイトの数値)をとった値として算出されている。式3で規定される暗号化鍵 k_e は、そのような第2の鍵算出用パラメータ Y_{a2} に自己の秘密鍵 k_b の値でべき乗し、その結果について $\bmod N_2$ をとった値として算出される。以上のように、暗号化鍵 k_e は、共通秘密鍵 k_s (第1の鍵算出用因子 g_2 と第2の鍵算出用因子 N_2 として使用)、自己の秘密鍵 k_b と、送信相手であるユーザU1の秘密鍵 k_a とを用いて算出される。

【0067】図7を再び、参照して受信信号処理部26の動作を述べる。

ステップ32：受信信号処理部26は暗号化鍵 k_e を算

鍵 k_b と、ユーザU1の秘密鍵 k_a とを用いて、送受信アンテナ32で受信したデータの暗号解読処理に使用する暗号化鍵 k_e を導出する。暗号化鍵 k_e の導出方法については、図8を参照して詳述する。

【0056】図8は暗号化鍵 k_e の導出方法を示すフローチャートである。

【0057】ステップ41：無線通信端末装置2の受信信号処理部26は、メモリに記憶されている共通秘密鍵 k_s と、自己の秘密鍵 k_b と、通信相手(送信相手)であるユーザU1の秘密鍵 k_a とをメモリから検索して読みだす。

【0058】ステップ42：受信信号処理部26は、下記演算を行う。

【0059】

$$\dots (4)$$

$$\dots (5)$$

秘密鍵 k_s の下位1バイトのデータ、すなわち、共通秘密鍵 k_s の(7-0)ビットのデータである。また、第2の鍵算出用因子 N_2 は共通秘密鍵 k_s の上位1バイトのデータ、すなわち、暗号化鍵 k_e の(15-8)ビットのデータである。

【0063】以上から明らかなように、本実施の形態においては、無線通信端末装置1で使用した第1の鍵算出用因子 g_1 と無線通信端末装置2で使用した第1の鍵算出用因子 g_2 とは同じである。同様に、無線通信端末装置1で使用した第2の鍵算出用因子 N_1 と無線通信端末装置2で使用した第2の鍵算出用因子 N_2 とは同じである。

【0064】ステップ43：受信信号処理部26は下記の演算により暗号化鍵 k_e を算出する。

【0065】

$$\dots (6)$$

出した場合、その暗号化鍵 k_e を用いて受信データを暗号解読する。暗号化鍵 k_e を用いるデータの暗号解読方法自体は公知の処理を適用できる。このようにして暗号解読された受信データが、図4のステップ7において、復号される。

【0068】上述した無線通信システムにおける情報の機密性について考察する。共通秘密鍵 k_s は無線通信システムを利用できる全てのユーザが知っている。しかしながら、無線通信システムのユーザであっても、通信を行わない他のユーザは通信を行ったユーザU1の秘密鍵 k_a およびユーザU2の秘密鍵 k_b を知らない。したがって、他のユーザがユーザU1とユーザU2の通信情報を受信したとしても、その暗号化鍵 k_e が不明なので、受信したデータを暗号解読できない。

【0069】無線通信システムを正当に使用しない第3者は、共通秘密鍵 k_s はもとより、ユーザU1の秘密鍵 k_a およびユーザU2の秘密鍵 k_b を知らない。したが

って、第3者がユーザU1とユーザU2の通信情報を傍受したとしても、その暗号化鍵 k_e が不明なので、受信したデータを暗号解読できない。共通秘密鍵 k_s は無線通信システムを利用するユーザ全員が知っているので、通信相手であるユーザU1とユーザU2の秘密鍵 k_a 、 k_b よりは機密性は低く、第3者が知る可能性は高い。しかしながら、第3者はユーザU1の秘密鍵 k_a およびユーザU2の秘密鍵 k_b を知らないで、暗号化鍵 k_e が判らず、傍受した信号を解読できない。さらに、第3者は、暗号化鍵 k_e が、共通秘密鍵 k_s とユーザU1の秘密鍵 k_a とユーザU2の秘密鍵 k_b を用いた式1~3の演算結果であることは判らない。したがって、この暗号化鍵 k_e は、無線通信システム内の通信を行わないユーザはもちろん、無線通信システムの利用者ではない第3者に対して高い秘匿性を有している。

【0070】その一方で、式1~3から判るように、無線端末装置における暗号化鍵 k_e の算出方法は比較的簡単である。したがって、無線端末装置における暗号処理を行う装置の構成は簡単である。

【0071】さらに、ユーザU1の秘密鍵 k_a およびユーザU2の秘密鍵 k_b を企業内無線LANを利用するユーザ同士で交換しただけなので、鍵交換に伴うユーザU1の秘密鍵 k_a およびユーザU2の秘密鍵 k_b の秘

密が暴露される可能性は低い。

【0072】ユーザU1の秘密鍵 k_a およびユーザU2の秘密鍵 k_b の交換方法について例示する。第1の方法は、無線通信を介さずに、たとえば、有線電話回線を用いた通信または電話連絡により、たとえば、MODEMを用いて、あるいは、パソコン通信を用いて、無線端末装置相互にユーザU1の秘密鍵 k_a とユーザU2の秘密鍵 k_b の交換を行う。このようにデータを送信する無線通信とは別の方法で鍵 k_a および鍵 k_b を交換することにより、鍵 k_a および鍵 k_b の漏洩の機密性は高まる。

【0073】さらに、そのようなユーザU1の秘密鍵 k_a およびユーザU2の秘密鍵 k_b の交換を、1日ごと、1週間ごと、あるいは1月ごとに更新するとより効果的である。比較的短期間に新たな鍵 k_a および鍵 k_b が交換されると、仮に、鍵 k_a および鍵 k_b のいずれかが漏洩した場合でも、第3者が暗号を解読しようとしても、そのときは新しい鍵 k_a および鍵 k_b によって暗号化されているので、傍受した信号を解読できない。したがって、その後、データの改ざんもできない。

【0074】鍵 k_a および鍵 k_b の更新期間が短いほうが、解読される可能性は非常に低くなる。たとえば、機密性の高い通信を行う場合は、極端な場合、その都度、鍵 k_a および鍵 k_b を更新する。特に、企業内無線LANあるいは家庭内無線LANの場合、送信相手は判っており鍵の交換は容易である。

【0075】鍵の交換が短期間で行われた場合、かりに、第3者が、上記式1~3のアルゴリズムを知得した

場合でも、解読した場合は更新された新たなユーザU1の秘密鍵 k_a およびユーザU2の秘密鍵 k_b を用いて暗号化されているので、第3者は実質的に解読できなくなる。

【0076】第2の方法は無線通信を介してユーザU1の秘密鍵 k_a およびユーザU2の秘密鍵 k_b の交換をすることである。ただし、この場合、第3者に傍受されたとき秘密鍵が知得されない対策が望ましい。そのような方法を例示する。第1の方法は、鍵 k_a および鍵 k_b を上記した方法で、既存のユーザU1の秘密鍵 k_a およびユーザU2の秘密鍵 k_b を用いて、暗号化して送出することである。既存の鍵 k_a および鍵 k_b が解読されない限り、新たな鍵 k_a および鍵 k_b の秘匿性は確保される。さらに好ましくは、そのような暗号化された鍵 k_a および鍵 k_b の挿入位置として、固定の位置ではなく、可変位置にすることである。暗号化された鍵 k_a および鍵 k_b の位置を示すデータも暗号化して送出する。

【0077】さらに好ましくは、第1の方法として上述したように、1日ごと、1週間ごと、1月ごとのように、あるいは、通信の都度、鍵 k_a および鍵 k_b の更新することである。

【0078】以下、図1とは異なる無線通信システムの構成例について述べる。

【0079】図9は本発明の無線通信装置および無線通信方法が適用される他の無線通信システムの構成例を示す図である。図9に図解した無線通信システムにおいては、無線通信端末装置A~Dが存在するが、無線通信端末装置AとB、無線通信端末装置CとDとが1対1で通信を行う場合に特定した例である。この場合も、共通秘密鍵 k_s が全ての無線通信端末装置に対して付与される。しかしながら、ユーザの秘密鍵の交換は、 $k_a : k_b$ 、 $k_c : k_d$ の対のように、通信相手のみに行われる。送信機10における暗号化鍵 k_e の算出、その暗号化鍵 k_e を用いた暗号処理、受信機20における暗号化鍵 k_e の算出、その暗号化鍵 k_e を用いた暗号解読処理は上述した方法で行われる。

【0080】この無線通信システムにおいて、無線通信端末装置AとB側と、無線通信端末装置CとD側とは、同じ無線通信システムに属していても、ユーザの秘密鍵が異なり、かつ、知らないで、かりに受信しても、互いに解読できない。このように、たとえば、同じ企業内無線LAN（家庭内無線LANも同様）に属していても、ユーザの秘密鍵を異ならせることにより、無線通信端末装置AとB側と、無線通信端末装置CとD側とは、互いに機密を保持した通信が可能となる。しかも、上述したように、通信相手とユーザの秘密鍵の更新を頻繁に行うことにより、同じ無線通信システムの他のユーザにとっても秘匿性の高い通信が可能となる。もちろん、第3者に対しては、無線通信システム内のユーザに対してよりもさらに高い機密性が維持できる。

【0081】図10は本発明の無線通信装置および無線通信方法が適用されるさらに他の無線通信システムの構成例を示す図である。図10に図解した無線通信システムにおいては、無線通信端末装置A～Dが存在するが、無線通信端末装置Aをキー無線通信端末装置として、他の無線通信端末装置B～Dが無線通信端末装置Aに1対1で接続されて通信する構成である。この場合も、共通秘密鍵 k_s が全ての通信相手となる無線通信端末装置A～Dに対して付与される。しかしながら、ユーザの秘密鍵の交換は、 $k_a : k_b$ 、 $k_a : k_c$ 、 $k_a : k_d$ の対のように、通信相手のみに行われる。送信機10における暗号化鍵 k_e の算出、その暗号化鍵 k_e を用いた暗号処理、受信機20における暗号化鍵 k_e の算出、その暗号化鍵 k_e を用いた暗号解読処理は上述した方法で行われる。

【0082】この無線通信システムにおいて、たとえば、無線通信端末装置AとBとが暗号処理通信を行っているときは、無線通信端末装置CとD側とは、ユーザの秘密鍵が異なり、暗号化鍵 k_e が異なるので、信号を受信しても解読できない。このように、たとえば、同じ企業内無線LAN（家庭内無線LANも同様）に属していても、ユーザの秘密鍵を異ならせることにより、無線通信端末装置AとB側と、無線通信端末装置CとD側とは、互いに機密を保持した通信が可能となる。しかも、上述したように、通信相手とユーザの秘密鍵の更新を頻繁に行うことにより、同じ無線通信システムの他のユーザにとっても秘匿性の高い通信が可能となる。もちろん、第3者に対しては、無線通信システム内のユーザに対してよりもさらに高い機密性が維持できる。

【0083】図11は本発明の無線通信装置および無線通信方法が適用される他の無線通信システムの構成例を示す図である。図11に図解した無線通信システムにおいては、無線通信端末装置A～Dが相互に1対1で接続されて通信する構成である。この場合も、共通秘密鍵 k_s が全ての通信相手となる無線通信端末装置A～Dに対して付与される。そして、ユーザの秘密鍵の交換は、通信相手ごとに行われる。送信機10における暗号化鍵 k_e の算出、その暗号化鍵 k_e を用いた暗号処理、受信機20における暗号化鍵 k_e の算出、その暗号化鍵 k_e を用いた暗号解読処理は上述した方法で行われる。

【0084】この無線通信システムにおいて、たとえば、無線通信端末装置AとBとが暗号処理通信を行っているときは、無線通信端末装置CとD側とは、ユーザの秘密鍵が異なり、暗号化鍵 k_e が異なるので、信号を受信しても解読できない。このように、たとえば、同じ企業内無線LAN（家庭内無線LANも同様）に属していても、ユーザの秘密鍵を異ならせることにより、無線通信端末装置AとB側と、無線通信端末装置CとD側とは、互いに機密を保持した通信が可能となる。しかも、上述したように、通信相手とユーザの秘密鍵の更新を頻

繁に行うことにより、同じ無線通信システムの他のユーザにとっても秘匿性の高い通信が可能となる。もちろん、第3者に対しては、無線通信システム内のユーザに対してよりもさらに高い機密性が維持できる。

【0085】本発明の無線通信装置および無線通信方法が適用される無線通信システムとしては、図1、図9～図11に図解した無線通信システムに限らず、種々の無線通信システムにも適用できる。

【0086】

10 【発明の効果】本発明の無線通信装置および無線通信方法によれば、比較的閉じられた無線通信システムにおいてそのユーザに共通秘密鍵を配付し、相互に通信相手が特定される無線通信端末装置相互に秘密鍵を交換し、これら共通秘密鍵とユーザ秘密鍵を用いて暗号化鍵を算出し、その暗号化鍵を用いてデータを暗号処理するので、機密性の高い無線通信が可能となる。

20 【0087】また、本発明の暗号化鍵算出方法は比較的簡単なので、無線通信端末装置および無線通信方法における処理の負担が軽い。換言すれば、本発明によれば、比較的簡単な演算で機密性の高い暗号化処理が可能となる。

【0088】さらに本発明によれば、ユーザ秘密鍵の交換および更新が容易なので、結果として、暗号化鍵を容易に変更することが可能となる。このことは機密性を高めることを意味している。

【図面の簡単な説明】

【図1】図1は本発明の無線通信装置および無線通信方法が適用される無線通信システムの構成例を示す図である。

30 【図2】図2は図1に図解した無線通信システムにおける無線通信端末装置の構成例を示す図である。

【図3】図3は図2に図解した無線通信端末装置の送信動作を示すフローチャートである。

【図4】図4は図2に図解した無線通信端末装置の受信動作を示すフローチャートである。

【図5】図5は図3に示した無線通信端末装置の送信信号処理部の動作のうち、暗号処理の概要を示すフローチャートである。

40 【図6】図6は図5に図解した処理のうち、暗号化鍵の算出方法の詳細を示すフローチャートである。

【図7】図7は図4に示した無線通信端末装置の受信信号処理部の動作のうち、暗号解読処理の概要を示すフローチャートである。

【図8】図8は図7に図解した処理のうち、暗号化鍵の算出方法の詳細を示すフローチャートである。

【図9】図9は本発明の無線通信装置および無線通信方法が適用される他の無線通信システムの構成例を示す図である。

50 【図10】図10は本発明の無線通信装置および無線通信方法が適用されるさらに他の無線通信システムの構成

例を示す図である。

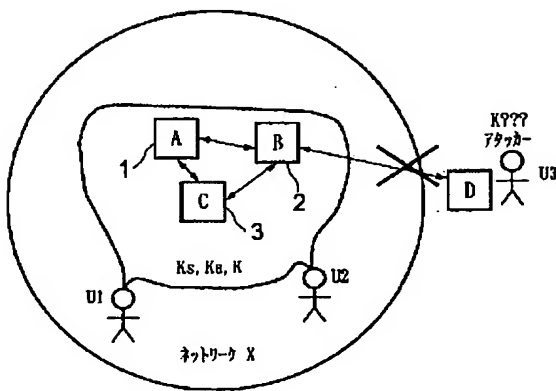
【図11】図11は本発明の無線通信装置および無線通信方法が適用される他の無線通信システムの構成例を示す図である。

【符号の説明】

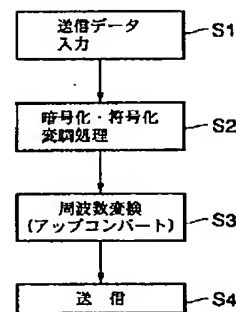
- 1・・・無線通信端末装置
10・・・送信機
12・・・送信データ入力部
14・・・送信信号処理部
16・・・周波数変換部
18・・・送信部

- 20・・・受信機
22・・・受信部
24・・・周波数変換部
26・・・受信信号処理部
28・・・復号信号出力部
30・・・共通部
32・・・送受信アンテナ
34・・・アンテナ切り換え部
36・・・送受信信号処理部
10 2～3・・・無線通信端末装置

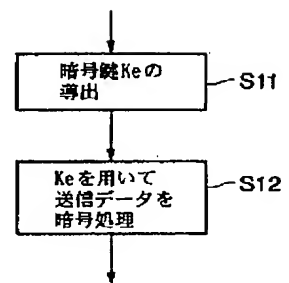
【図1】



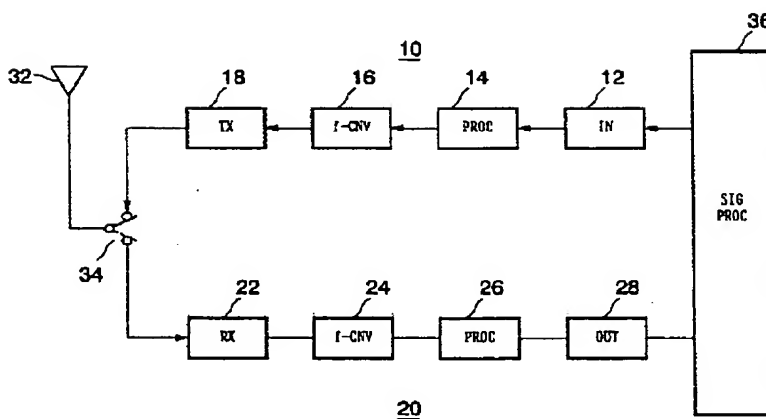
【図3】



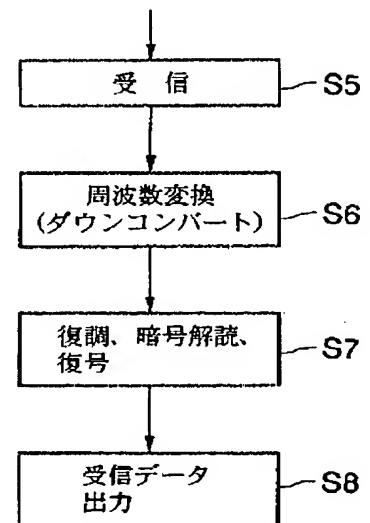
【図5】



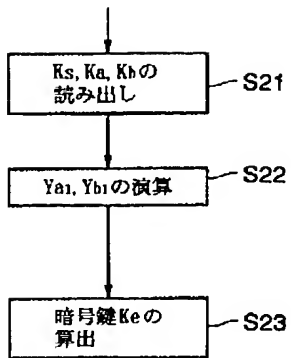
【図2】



【図4】

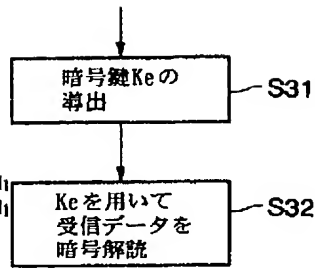


【図 6】

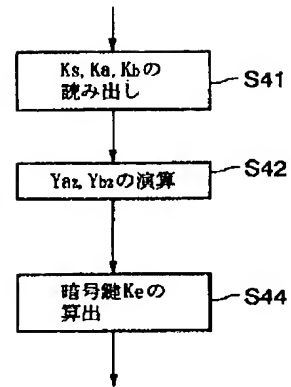


$$\begin{aligned}
 Y_{a1} &= (g_1^{K_a}) \bmod N_1 \\
 Y_{b1} &= (g_1^{K_b}) \bmod N_1 \\
 g_1 &= Ks(7-0) \\
 N_1 &= Ks(15-8) \\
 K_e &= (Y_{b1}^{K_a}) \bmod N_1
 \end{aligned}$$

【図 7】

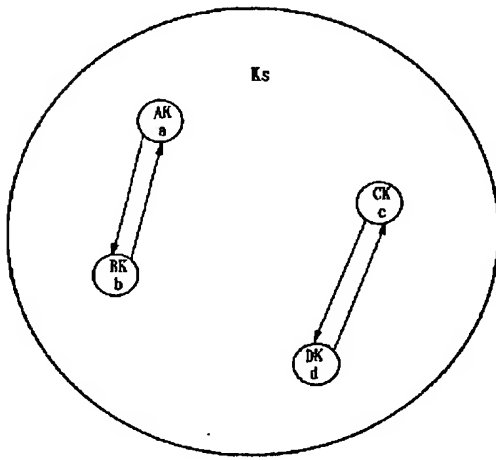


【図 8】

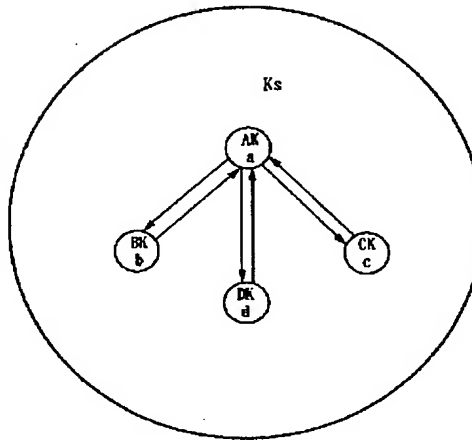


$$\begin{aligned}
 Y_{a2} &= (g_2^{K_a}) \bmod N_2 \\
 Y_{b2} &= (g_2^{K_b}) \bmod N_2 \\
 g_2 &= Ks(7-0) \\
 N_2 &= Ks(15-8) \\
 K_e &= (Y_{b2}^{K_b}) \bmod N_2
 \end{aligned}$$

【図 9】



【図 10】



【図 11】

